Enabling roaming across heterogeneous IoT wireless networks

Torroglosa-Garcia, Elena M.; Alcaraz Calero, Jose M.; Bernal Bernabe, Jorge; Skarmeta, Antonia

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2020.2998416

E-pub ahead of print: 28/05/2020

Document Version
Peer reviewed version

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Enabling Roaming across Heterogeneous IoT Wireless Networks: LoRaWAN meets 5G

ELENA M. TORROGLOSA-GARCIA[1], JOSE M. ALCARAZ CALERO [1], JORGE BERNAL BERNABE [2] AND ANTONIO SKARMETA [2],

[1]School of Computing, Engineering and Physical Sciences, University of West of Scotland, United Kingdom (e-mail: elena.torroglosa, jose.alcaraz-calero@uws.ac.uk)

[2]University of Murcia, Spain (e-mail: jorgebernal, skarmeta@um.es)

Corresponding author: Elena Torroglosa-Garcia (e-mail: elena.torroglosa@ uws.ac.uk).

This work has been funded by a grant for postdoctoral training and improvement abroad, funded by the Ministry of Employment, Universities, Enterprise and Environment of the CARM©, through the Seneca Foundation-Agency for Science and Technology of the Region of Murcia (Spain). This work has been also partially supported by the European Commission H2020 5G-PPP ICT-2016-2 SliceNet project GA 761913, as well as H2020 European project INSPIRE-5Gplus GA 871808.

ABSTRACT Despite the latest research efforts to foster mobility and roaming in heterogeneous Low Power Wide Area Networks (LP-WANs) networks, handover roaming of Internet of Things (IoT) devices is not a success mainly due to fragmentation and difficulties to establish trust across different network domains as well as the lack of interoperability of different LP-WANs wireless protocols. To cope with this issue, this paper proposes a novel handover roaming mechanism for Low Range Wide Area Network (LoRaWAN) protocol that relies on the trusted 5G network to perform IoT device's authentication and key management, thereby extending the mobility and roaming capabilities of LoRaWAN to global scale. The proposal enables interoperability between 5G network and LoRaWAN , whereby multi Radio Access Technologies IoT (multi-RAT IoT) devices can exploit both technologies interchangeably, thereby fostering novel IoT mobility and roaming use cases for LP-WANs not experimented so far. Two integration approaches for LoRaWAN and 5G have been proposed, either assuming 5G spectrum connectivity with standard 5G authentication or performing 5G authentication over the LoRaWAN network. The solution has been deployed, implemented and validated in a real and integrated 5G-LoRaWAN testbed, showing its feasibility and security viability.

INDEX TERMS 5G mobile communication, LoRaWAN, Internet of Things, Roaming, Authentication

I. INTRODUCTION

It is foreseen that Internet of Things (IoT) scenarios based on wireless massive Machine-Type Communications (mMTC) [1], will scale up to billions of heterogeneous connected devices in the coming years [2]. The mMTC ecosystem is composed of a plethora of different kinds of wireless technologies. On the one hand, Low-Power WAN Area Networks (LP-WAN) networks such as LoRa/LoRaWAN [3] and SigFox [4], each one featuring different functionalities, data patterns, and capabilities. On the other hand, 3GPP cellular networks have improved its support on mMTC in the latest 5G releases [5] compared to previous Long-Term Evolution (LTE) versions, including Narrowband Internet of Things (NB-IoT) [6] and LTE-M protocols, although they still yet lacks of some capabilities supported by other cheaper non-cellular LP-WAN (Low-Power WAN Area Networks) networks, such as efficient treatment of sporadic patterns, and short packet transmissions [7].

In particular, LoRaWAN, that falls in LP-WAN category [8], is gaining a global momentum and expansion mainly due to the open-license and economic model as well as the usage of unlicensed spectrum, which makes it accessible for everyone [9]. Both, LoRaWAN and 5G IoT wireless technology are complementary and widely used, but not yet inter-operable.

This heterogeneity in the IoT wireless landscape is one of the major challenges to be faced in up-coming years, since each wireless protocol has its own network mechanisms,

including authentication protocols, that has led to a high fragmentation and silos of different kinds of IoT networks. To cope with these issues, some initial ongoing efforts such as those being accomplished by the IETF working group *IPv6* over LP-WAN, are dealing with inter-operability across heterogeneous LP-WAN networks, proposing new adaptations and network protocols but mainly for OSI layer 3 and layer 4.

Certain use cases like those derived from Intelligent Transport Systems (ITS), including the deployment of vehicles like trucks, ambulances or drones in different scenarios, can benefit from the existence of roaming mechanisms. Notice that in LoRaWAN, roaming is understood as end-device mobility across different LoRaWAN administrative domains, regardless of whether it is in the same country or not. These mobility ITS scenarios imposes specific constrains in terms of low latency and high bandwidth. In principle, these use cases are not fully suitable for LP-WAN communications, which are characterized by low data rates, high latency and low power features. However, LP-WANs also enables several IoT use cases based on mMTC communications, and there are certain IoT mobility use cases that could be perfectly addressed by LP-WANs, and therefore, supporting handover roaming in these networks is highly desirable. For instance, fleet controlling to collect and send operating data of wagon vehicles could be supported by roaming among LP-WANs IoT networks.

In this sense, since version LoRaWAN version 1.1 [3], the LoRaWAN architecture provides support for a simple handover roaming across different LoRaWAN networks. This is an initial approach to address the inter-operability between networks. However, the LoRaWAN roaming requires explicit agreement negotiations between different administrative domains, in ad-hoc manner, case by case, exchanging sensitive security information. This makes roaming very difficult in practice, mainly due to the lack of trust between different peers. On the other side, roaming is widely supported for the cellular IoT networks such as LTE-M and NB-IoT using the control plane of the 4G and 5G networks. However, these solutions are always trying to provide support for deployments among homogeneous technologies, being mainly motivated by industrial-centric interests to make a concrete technologies leading in the IoT sector. This situation leaves aside more impacting user-centric approaches based on the enabling of roaming capabilities between heterogeneous IoT networks deployed using different technologies in order to allow to best possible use of technology for the final users making use of multi-interface IoT devices.

To address this challenge, this research work has devised, implemented and validated a novel handover roaming capability for LoRaWAN that relies on the 5G architecture to enlarge the LoRaWAN roaming scope and its authentication scheme to global scale. Our approach relies on the existing 5G identity management service, AAA and its underlying federation, as a trusted network service to perform the authentication of IoT devices in roaming LP-WAN networks. In particular, the solutions leverage the current authentication and key management processes in LoRaWAN integrating them with the 5G authentication mechanism.

The novel solution proposed herein enables handover roaming across different domains in heterogeneous wireless networks technologies, i.e. LoRaWAN and 5G, thereby opening new possibilities and IoT use cases not experimented until now. Thus, multi-RAT IoT devices endowed with both, 5G and LoRaWAN user equipment's can use them interchangeably, enabling the usage of the efficient and cheaper LoRaWAN network equipment in visited domains where there are not pre-established LoRaWAN agreements, using SIM-based authentication in the 5G network through the LoRaWAN protocol.

The proposed roaming architecture brings the following innovations:

1) It extends the use of the advanced roaming services provided by 5G cellular networks into LoRaWAN networks.
2) It delegates the ad-hoc management of trust relationships in LoRaWAN networks to a third party that will provide a common and trusted identity management.
3) It leverages the 3GPP services provided under the umbrella of 5G networks with the new non-3GPP connectivity services associated to LoRaWAN IoT networks.

The rest of this paper is structured as follows. Section III provides a background on both LoRaWAN and 5G, and specifically to the security and AAA aspects. Section IV is devoted to analyse the current related works. Section V is the core of the paper and provides and analyses two different approaches for enabling roaming in LoRaWAN with 5G. Section VI analyses the security of the proposed roaming approaches. The proof of concept implementation to validate the solution as well as and the empirical results are described in section VII. Finally, Section VIII concludes the paper.

II. MOTIVATION

The arrival of the Internet of Things entails new scenarios and business models related to communication between devices and to the use and commercialization of necessary communication infrastructures. The integration between cellular networks and different radio-access technologies, including unlicensed spectrum (such as LoRaWAN) is a hot topic being part of the working items defined in the incoming future 3GPP Rel 16 and 17. The incorporation of different types of devices, both fixed (electrical appliances, smart bulbs, industrial machinery, urban furniture) and mobile (vehicles, mobiles, parcels, clothing and accessories, etc.) makes the use cases more and more varied and complex.

To provide connectivity to these scenarios, it is necessary to have powerful, robust and extensive networks, and offering flexible connectivity mechanisms to operators is an interesting solution. Roaming is a mechanism that allows the mobility of devices between different domains (from its home domain to another available) allowing to improve the coverage (sharing antennas to reduce the densification),

device mobility while transmitting in areas with low coverage (tracking services) and mobility across multiple networks, within a given country, internationally or between private and public ones.

These new opportunities of roaming between networks of different domains can grew exponentially if we consider the integration between different technologies, thanks to multi-RAT IoT devices, to take advantage of the best part of each one. In particular, the integration of the LoRaWAN networks that offer long range coverage, low power requirement and high scalability in the number of devices with the solid and extended back-end of 5G operators. This model allows building new strategies. On the one hand, any 5G network operator will be able to extend business influence to cover LoRaWAN networks. On other hand, any LoRaWAN network operator will be able to extend the potential users of their infrastructure and monetize their usage by relying on the trust relationship with 5G operators. This creates a win-win situation. There is a big advantage of delegating the device roaming to 5G operators, which usually have bigger back-end and have an already established trusted federation to perform roaming between infrastructures, and in fact, they offer these kind of services to virtual operators.

III. BACKGROUND

A. LORAWAN

LoRaWAN [3] is a LP-WAN protocol specification that describes the network protocols to inter-connect wireless network that make use of the LoRa physical wireless interface [10], which is an scalable bandwidth modulation based on Chirp Spread Spectrum (CSS).

Figure 1 depicts the most significant characteristics of LoRaWAN networks (as example of a LP-WAN network) in contrast to LAN and cellular networks [11].

LoRaWAN is a low cost, high capacity, low power and long range protocol, that, unlike other LP-WAN technologies, allows to customize several network options to fine-tune performance [12], making the network protocol fairly adaptable. LoRaWAN is an asymmetric protocol, with a star topology, where devices are connected directly to a gateway, which in turn, are connected to a LoRaWAN Network Server (NS) that acts a controller of the network. The standard defines three kinds of classes according to the three types of devices capabilities. Class A is intended for constrained devices, energy-limited devices, with bi-directional communication but very limited downlink capacity. In Class B the protocol defines an scheduling mechanism for devices to receive improved downlink messages, which imposes additional energy consumption. Finally, Class C allows keeping the reception windows open, even when devices are transmitting, in order to achieve low-latency communications.

Regarding LoRaWAN security, the protocol defines two device activation methods LoRaWAN Over-The-Air Activation (OTAA) and Activation By Personalisation (ABP). In the ABP mode, either the manufacturer or the application manager adds the cryptography keys in the end-devices and the Network Server. On the other hand, in OTAA activation mode (LoRaWAN 1.1), the keys are generated through exchange of join messages (join-accept and join-request) between the device, the NS and the Join Server, as shown in steps 1 and 2 of figure 2. The Message Integrity Code (MIC) in the join-request allows authenticating the device, as the MIC is generated making use of the device root key $NwkKey$. In particular, the function to calculate MIC value for the *JoinRequest* header field is:

$$\begin{aligned} cmac =& aes128\_cmac(NwkKey, MHDR|JoinEUI| \\ & DevEUI|DevNonce) \\ MIC =& cmac[0..3] \end{aligned}$$

Then, the device derives the session keys ($FNwkSIntKey$, $SNwkSIntKey$ and $NwkSEncKey$), with aes-128, using as baseline the predefined $NwkKey$ root keys, while $AppSKey$ is derived using $AppKey$ root key. All the derivation functions also use the information exchanged in the join messages, including the $DevNonce$ and the $JoinNonce$ and $JoinEUI$ both generated by the Join Server.

The $FNwkSIntKey$ is used to generate the MIC of uplink messages, $SNwkSIntKey$ is employed to generate downlink MICs, and $NwkSEncKey$ is used to encrypt the MAC payloads between the device and the NS using AES-128. AES-CMAC (Cipher-based Message Authentication Code) is used to generate the MIC and provide integrity and authentication. In addition, LoRaWAN features another channel protection capability at application layer, over the LoRaWAN NS. In this sense, the AppKey (plus join material) is used to derive the Application session Key $AppSKey$ that is used to encrypt and decrypt the application payloads between the device and the application server (AS).

For further analysis on LoRaWAN security and associated issues, the reader is referred to this paper [13].

As it will be seen in the following section, that reviews the 5G authentication and authorizations mechanism, the LoRaWAN security architecture is not ready for its integration with the extensible Authentication services that are provided by the 5G network to provide connectivity with other radio interfaces, e.g. WiFi Calls.

Regarding LoRaWAN roaming, LoRaWAN back-end specification [14] defines passive and handover roaming mechanisms to manage the movement of the LoRaWAN end-device between different Network Servers, being a requirement that each operator are configured with a roaming policy agreement that can individually allow/disallow the roaming with other network operators identified by their NetIDs.

B. 5G NETWORK

5G Networks are cellular networks based on 3GPP release 15 specification [15] that includes the complete definition of all the architectural components, interfaces and protocols of the cellular infrastructure. From 3GPP release 13 it also provides support for IoT devices using the both LTE-M and NB-IoT specifications. LTE-M is the simplified industry term for the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

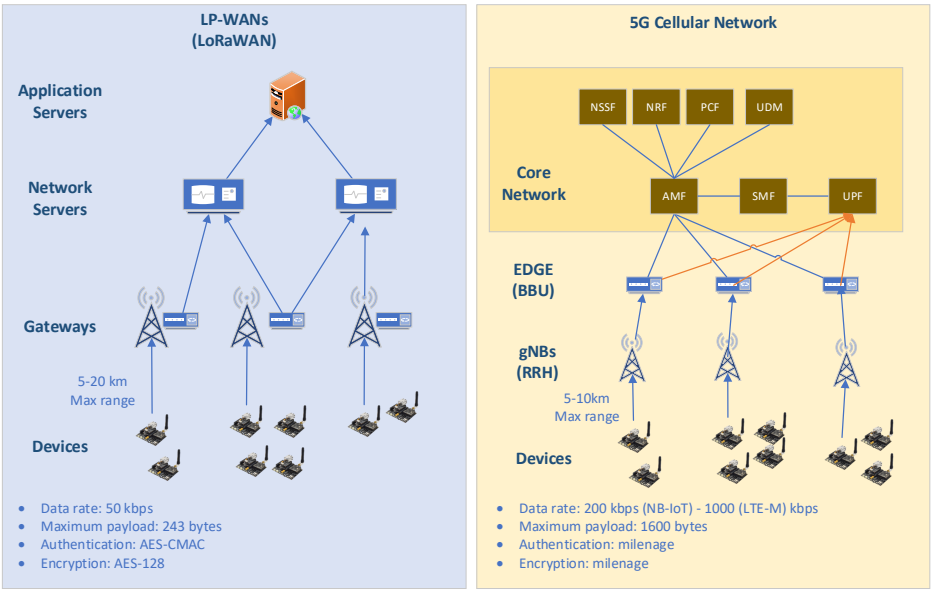

FIGURE 1. LPWAN vs 5G cellular networks overview

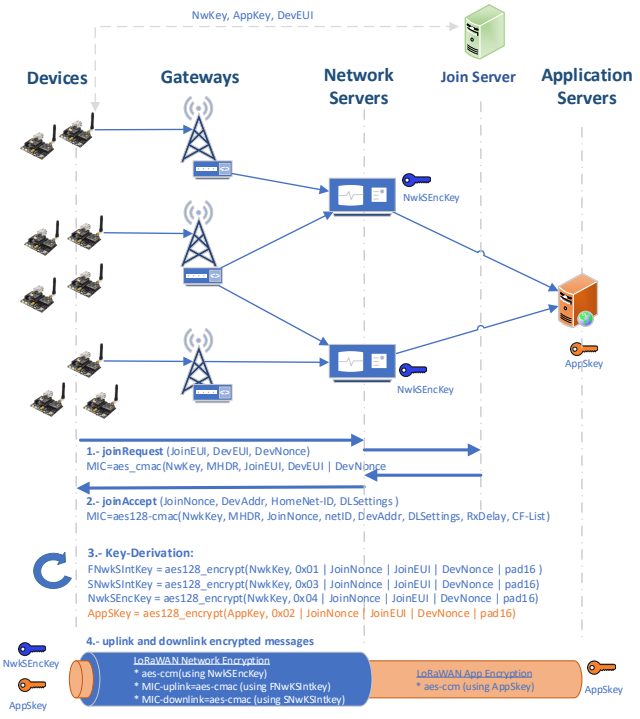

FIGURE 2. LoRaWAN: Security scheme Overview

LTE-MTC (Machine Type Communication) low power wide area network (LP-WAN). Narrowband Internet of Things (NB-IoT) is also defined in the same specification (rel 13) as a LP-WAN that focuses specifically on indoor coverage, low cost, long battery life, and high connection density. It uses OFDM modulation for downlink communication and SC-FDMA for uplink communications.

The 5G radio interface is an asymmetric protocol, with a star topology, where devices are connected directly to a Distributed Unit (DU) acting as a transceiver for the radio signals, which in turn, are connected to a (Centralized Unit) that acts a controller of the radio interface. The infrastructure is connected to the Evolved Packet Core, clearly separating the data links and control links. The User Plane Forwarder (UPF) is the component that received all the traffic of the final users in order to direct it to the internet or back to other users of the network. In the control plane, the access and mobility management function (AMF) is in charge of dealing with the mobility of the session along the different handovers of the user. The session management function (SMF) is in charge of maintaining the existing sessions. Also, the authentication server function (AUSF) is in charge of performing the authentication of the users on the network. The reader can see an overview of a 5G network layer on Figure 8.

5G networks, through the 5G Core (5GC) can interconnect and/or interwork when users roaming onto a network different to their Home Public Mobile Network (HPMN). This will be applicable when New Radio or eLTE (evolved LTE) radio bearers are used, connected to a 5GC, and both UE and visited PMN have matching capabilities. In the world of cellular networks, such as 5G and 4G, the term roaming is usually associated with the mobility of a device between countries, but this does not necessarily have to be the case, and roaming may simply mean the change from a home domain to a new visited domain. More details about 5G roaming technical guidelines are detailed in [16].

With respect to 5G security, authentication in the network is carried out using both an identity and a cryptography key [17]. About identification, a SUPI is a 5G globally unique Subscription Permanent Identifier (SUPI) allocated to each

subscriber and defined in 3GPP specification TS 23.501 [18]. The SUPI value is provisioned in USIM and UDM function in 5G Core. A Valid SUPI can be either of the following, an IMSI (International Mobile Subscriber Identifier) or a NAI (Network Access Identifier) as defined in RFC 4282 [19] based user identification as defined in TS 23.003 [20] for non-3GPP RAT. The IMSI (International Mobile Subscriber Identity) is a unique identification of the subscriber associated with all GSM, UMTS and LTE, 5G network SIM cards. It is stored as a 64 bits field and is sent by the phone to the network. IMSI consists of three parts:

- MCC - Mobile Country Code, first three digits. MCC uniquely identifies the mobile subscriber's home country.
- MNC - Mobile Network Code, 2 digits (European standard) or three digits (North American standard). The length of the MNC depends on the value of the MCC.
- MSIN - the remaining digits are the Mobile Subscription Identification Number (MSIN) within the network's customer base.

SUPI should not be transferred in clear text over 5G RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC). Therefore, in many cases it is used a one-time use subscription identifier, called The SUbscription Concealed Identifier (SUCI), which contains the concealed subscription identifier, e.g. the MSIN part of SUPI, and additional non-concealed information needed for home network routing and protection scheme usage. Based on home operator's decision, indicated by the USIM, the calculation of the SUCI shall be performed either by the USIM or by the ME

The Authentication key (K_i). The K_i is a 128-bit value used in authenticating the SIMs on a GSM mobile network (for USIM networks - 5G and 4G - you still need K_i but other parameters are also needed). Each SIM holds a unique K_i assigned to it by the operator during the personalisation process. The K_i is also stored in the Unified Data Management (UDM)) on the carrier's network.

The USIM card is designed to prevent someone from getting the K_i by using the smart-card interface. To do so, the USIM card provides a function that run the authentication algorithm to sign the data passed by the phone using the K_i. This, by design, makes using the USIM card mandatory unless the K_i can be extracted from the USIM card, or the carrier is willing to reveal the K_i.

The authentication process is described in a simplified way as follows:

1) When the mobile equipment starts up, it obtains the SUPI/IMSI from the USIM card, and passes this to the AUSF via AMF, requesting access and authentication. The mobile equipment may have to pass a PIN to the USIM card before the SIM card reveals this information.
2) AUSF searches then its UDM database for the incoming IMSI and its associated K_i.
3) The UDM then generates a random number (RAND, which is a nonce) and the AUTN token and signs both with the K_i associated with the SUPI/IMSI (and stored on the SIM card), computing another number, that is split into the Signed Response 1 (SRES, 32 bits) and the encryption key CK (64 bits).
4) The AUSF receives UDM authentication vector and then sends the RAND and the AUTN to the mobile equipment, which passes them to the USIM card. The SIM card checks the AUTN token and the SQN number encoded inside, and if it is right, produces the RES value and CK using to sign the K_i. It stores them and passes RES to AUSF.
5) The AUSF then compares its computed SRES with the computed RES that the mobile equipment returned. If the two numbers match, the SIM is authenticated and the mobile equipment is granted access to the operator's network. CK is used to encrypt all further communications between the mobile equipment and the network.

In [21] authors review the 5G authentication and authorization mechanism as well as associated security issues and recommendations.

IV. RELATED WORK

Roaming in LoRaWAN allows exchanging information among different LoRaWAN networks, but it is not yet a success as it is a peer to peer roaming mechanism, that requires high number of bilateral contracts between private-public LoRaWAN deployments, which makes it cumbersome to build trust. LoRaWAN alliance proposes a centralized roaming hub that allows scaling, but its feasibility is uncertain, as everyone needs to blindly trust within that central authority, and in turn, implicitly trust the members of the hub, in addition the contract agreements becomes more complex. Relying on 5G networks and their established telco agreements for cross-domain handover roaming in LoRaWAN, can facilitate the trustworthiness matters.

As it is highlighted in this important survey [22] on 5G Networks for the IoT, a major challenge in machine-type communications (MTC) (everything, anywhere and at anytime) is the seamless end-to-end interoperability between the different IoT radio network technologies used by heterogeneous IoT devices.

In [23] authors propose a integration of LoRaWAN with 4G/5G mobile networks, where the LoRaWAN gateway is modified to act as combination of User Equipment (UE) and eNB to interact with the Evolved Packet Core (EPC) in the Cellular network. Therefore, the User dataplane includes the EPC between the LoRaWAN Gateway and the LoRaWAN Network Server. Thus, the 5G networks acts as a transport mechanism to transmit LoRaWAN packets. Unlike in that paper, our approach does not require every LoRaWAN packet in the dataplane to go through the 5G Cellular network. In addition, that proposal does not allow to establish roaming

connectivity of LoRaWAN devices in visited LoRaWAN networks, as proposed in our work.

In [24], authors identifies 4 different ways of integrating LoRaWAN in 5G networks: 1) 3GPP access connectivity in the LoRaWAN Gateway, i.e. LPWAN packets added to LTE traffic, 2) LPWAN packets added to WiFi traffic, 3) eNB integration (LPWAN packets added to users' traffic), 4) external (LPWAN traffic does not affect EPC core network). However, none of these modes addresses the challenge of roaming in LoRaWAN, and therefore does not allow seamless connection of LoRaWAN devices in other foreign domains by relying on the 5G network, as it is done in our proposal.

Neumann et al. [25] proposed different models for the integration of 5G networks in industrial networks such as IEEE Time-Sensitive Networking (TSN) 802.1. On the other hand, 5G in 3G-ppp release 15 [15] supports non-3GPP access (WIFi) to the 5G Core. It supports access-agnostic authentication. In Non-3GPP access, during network registration the UE uses an N3IWF (instead of a Cellular gNB), and establishes a IPsec Security Association (SA) using IKE and EAP. The N3iWF acts as a EAP Proxy between UE and AUSF (Authentication Server Function). The UE performs the EAP-AKA' [26] authentication that ends-up with a session key for the tunnels. The N2 interface defines the control plane signalling between the access network and the 5GCN. Later on, the N3IWF uses N3 tunnels for transmitting user-plane PDUs towards the UPF (User Plane Function). However, our solution is not intended to use the 5G user plane to transmit the LoRaWAN packets, but rather it defines the authentication procedures that allow the usage of 5G authentication mechanism as baseline for LoRaWAN join procedures, where the IoT user datapath is thereafter transmitted through the LoRaWAN network. In addition, 3GPP release 16 might integrate WLAN systems in 5G using a "trusted model" called Trusted WLAN Access Network (TNAN), where the WIFI might be managed by a third-party trusted by the 5G operator.

An authentication service aimed to achieve interoperability among heterogeneous LP-WANs is proposed in [27]. The solution is independent of the type of LP-WAN technology and integrates the usage of AAA infrastructures and the Extensible Authentication Protocol (EAP) over CoAp in order to enable cross domain authentications. The solution generates corresponding LoRaWAN key material after successfully EAP authentication. Nonetheless, unlike our work, they do not consider the usage of the 5G network (and its AAA mechanisms) as enabler for handover roaming in LP-WAN networks.

This paper is the first novel work that takes advantage of the already existing mobility and roaming capabilities and trust established in 5G network in order to enable world-wide hand-over roaming across LoRaWAN networks. Enabling universal roaming in LoRaWAN would increase device provisioning across networks, permitting valuable use cases such as location of end-devices across different networks.

V. PROPOSED LORAWAN-5G INTEGRATION APPROACHES

There are different architectural approaches to perform the integration between LoRaWAN and 5G networks. They are determined by physical decisions (deployments, connectivity), logical decisions (APIs and Interfaces) and by trust relationships and administrative agreements between different domains. These scenarios enable new possibilities to develop future IoT applications.

The proposed scenario considers a LoRaWAN device that is deployed in a visited LoRaWAN network where there is no roaming agreement with its home LoRaWAN network. In the current scenario, the LoRaWAN device will not simply be able to connect into the visited LoRaWAN Network. To address this challenge, authors propose to use an alternative interface that integrated the LoRaWAN architecture to the 5G architecture to carry out the authentication of the LoRaWAN device using the 5G infrastructure as a common trusted entity to get access to the network.

As seen in Section III-A, LoRaWAN back-end specification [14] defines different roaming solutions to manage the movement of the LoRaWAN end-device from different known domains, being a requirement that each operator are configured with a roaming policy that can individually allow/disallow the roaming with other network operators identified by their NetIDs. Large telecommunication companies behind 5G, such as Orange and Swisscom [28] [29], among others, are also involved in other kind of non-cellular networks, infrastructures and services, and LoRaWAN is a clear example of IoT coverage being supported by them. In this scenario, it could be easy to take advance of their positioning to allow the simplification in the configuration of roaming not only among their different networking technologies but also between a very large number of small LoRaWAN networks by making use of the existing federation agreements that are currently available in their global cellular support.

A. GENERAL ARCHITECTURE

The proposed architecture integrates 5G and LoRaWAN architectures with the aim of achieving interoperability to provide support for roaming across different LoRaWAN networks thanks to the authentications and authorizations mechanisms provided by the 5G networks. To do so, it is proposed a new interface (and its API) between the Join Server in charge of the authentication and authorization of LoRaWAN devices and the UDM server used for the same purpose for 5G devices. The final objective is to delegate the LoRaWAN device authentication and authorization to the 5G infrastructure, which can validate the device's 5G credentials and make use of the answer to perform the decision on LoRaWAN networks.

Figure 3 depicts a multi-RAT IoT device with two different interfaces: 5G (named User Equipment - UE) and LoRaWAN (End Device - ED). The IoT device is moved from its home LoRaWAN network to a new visited network, where there

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

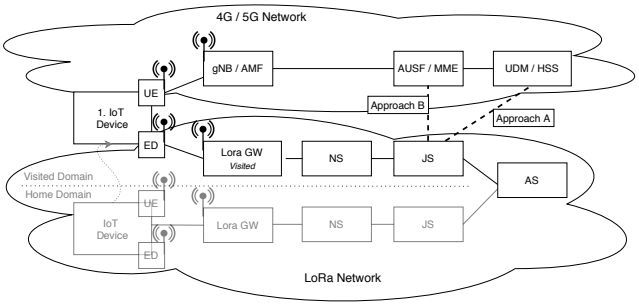

FIGURE 3. Integrated proposed architecture.

is not any existing roaming agreement. In a normal IoT scenario, the device would lose LoRaWAN connectivity.

The two approaches (apart from the already existing LoRaWAN roaming capabilities) have been proposed to allow the device to connect to the visited LoRaWAN network. On the one hand, the first approach considers that the visiting device has already an established and existing 5G session, implying the existence of 5G coverage. In such a case, the cryptographic session material (session keys) can be accessed and used by the IoT device to sign and protect LoRaWAN messages. It simplifies the integration and implementation of the solution.

On the other hand, the second approach considers that there is not any existing 5G session either because the interface is disabled to save energy or because there is a lack in the coverage of the 5G network. In such a case, the IoT device has only access to the 5G credentials available in the USIM: SUPI identifier and cryptographic functions. In this case, the integration between both network architectures is more complex and will require the modifications of some LoRaWAN messages. Both proposals are explained in detail in the following subsections.

B. APPROACH A: LORAWAN INTEGRATION WITH 5G AUTHENTICATION SERVICES

This proposal assumes that a multi-RAT IoT device with a dual-interface, LoRaWAN and 5G connectivity is deployed in a visited LoRaWAN with no LoRaWAN roaming agreements. The IoT device does not have 5G coverage in its radio interface but it have access to the information and functions available in the USIM using by such cellular interface. In this context, the IoT device can make use of the existing 5G credentials available in the USIM to authenticate the IoT device using the LoRaWAN connectivity in order to be authorized and accounted into such LoRaWAN network. As previously described in section III-A, the LoRaWAN specification performs device authentication based on a pre-shared key that is used to calculate the MIC field (a hash field in the message header) included in every sent LoRaWAN packet but specially in the initial *JoinRequest* message. This message is used to authenticate the LoRaWAN device, without any other initial negotiation or processing of any challenge data from the infrastructure. This implies a great change

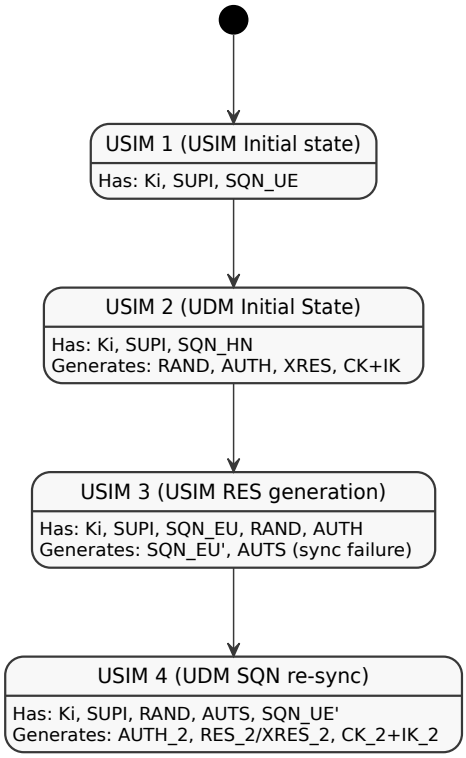

FIGURE 4. State diagram of 5G authentication key derivation at the USIM.

compared to the authentication workflow carried out in 5G and other common authentication mechanisms.

When the IoT device trying to authentication using its LoRaWAN cryptographic information into the visited network, it will fail since there is not any roaming relationship between the LoRaWAN device and the new visited LoRaWAN network. At this moment, we do propose to do not fail and stop, and rather, try the LoRaWAN authentication based on 5G credential. For this aim, authors propose two key innovations. First, to make use of the USIM authentication information in the LoRaWAN network and to extend the join server to allow the delegation of the authentication into the 5G infrastructure, thanks to a trust relationship established between the LoRaWAN network and the 5G network operator. This trust relationship will allow to make use of the UDM 5G services to carry out the authentication and use the response to perform the validation of the first LoRaWAN message (*JoinRequest*).

In the 5G-AKA authentication [15], session keys are derived from a pre-shared key (K_i) and some data ($RAND$, $AUTN$) received from the infrastructure during the authentication process. The 5G cryptographic information and authentication vectors are calculated in both USIM and in the UDM service available in the 5G infrastructure but all the authentication process is initiated and enforced by the AUSF server. Thus, architecturally, the interface between networks has been designed via AUSF component but the security steps are logically done between USIM and UDM.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

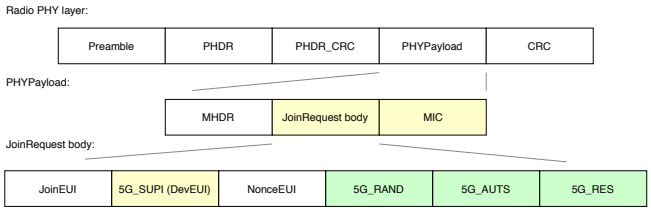

FIGURE 5. Extended Join Request frame to contain 5G authentication data.

Figure 4 depicts what are the initial data owned by each entity and what data is interchanged and generated at each step of the complete authentication steps. At the beginning, UDM generated $RAND$, $AUTN$, $XRES$ and $CK + IK$ keys (see step 2 in Figure 4). It sends both $RAND$ and $AUTN$ to the USIM as a challenge. The USIM then generated directly $RES, CK + IK$ using such received information, it allows to authenticate they network by the SIM card. Then, RES is sent back to the UDM and if it matches with its calculated $XRES$, authentication of the UE in the network will be positive and they have the session keys (CK and IK already shared), used as encryption and integrity keys, respectively. (see step 4 in Figure 4). The USIM can be or not synchronized with the infrastructure with respect to sequence numbers (SQN), i.e. SQN_UE is equal to SQN_HN. The $AUTS$ value is used as a standardized inter-medium step to perform such synchronization of sequence numbers. Thus, to make sure both are synchronized, they can decide to share such $AUTS$ value rather than their sequence number to avoid replay attacks and at the same time avoid any synchronization problem. (see step 3 in Figure 4). After the synchronization, the normal authentication process explained is re-executed.

The proposed solution consists on generating all the 5G authentication information inside the USIM, even some part that is traditionally carried out in the network, including the synchronization steps, to make sure that USIM and UDM service could share the same cryptography information. From all the steps previous described, the minimum required parameters to allow UDM to validate the process carried out by the USIM and therefore authenticate the device are $RAND$, $AUTS$ and RES. RES will be used as a proof of key possession, $RAND$ will be used as a shared seed for the challenge and $AUTS$ will be used to ensure synchronization. Our proposal is to send this information inside of the initial LoRaWAN *JoinRequest* message. It implies extending the fields included in the LoRaWAN *JoinRequest* message with such fields, $RAND$, $AUTS$ and RES as depicted in Figure 5 and to make the calculation of the MIC value using the approach of the standard method but including as well these newly inserted values.

Figure 6 shows a detailed sequence diagram of all the interactions proposed in this integration approach. Message 1 shows how initially the IoT device tries to access with a normal LoRaWAN *JoinRequest* message, but since it is a visited LoRaWAN network and the LoRaWAN device is not registered, these message are discarded. After several retries, the new 5G-LoRaWAN roaming mechanisms is activated.

Messages 2 to 3 are carried out inside the IoT device between the LoRaWAN device and the 5G USIM component to generate all required 5G keys and data explained in the previous paragraphs (Figure 4), as result of the emulation of the whole information exchanged and generated in the standard authentication process. At this point, CK and IK are keep as session keys in the USIM. After that, step 4 generates the LoRaWAN MIC making use of the IK key as LoRaWAN Network Key. Message 5 and 6 represents the new LoRaWAN *JoinRequest* extended to include $RAND$, $AUTS$ and RES fields along with the standard fields, and newly calculated MIC.

$$\begin{aligned} cmac =& aes128\_cmac(NwkKey, MHDR|JoinEUI| \\ & DevEUI|DevNonce|RAND|AUTS|RES) \\ MIC' =& cmac[0..3] \end{aligned}$$

When this message is received by the LoRaWAN Join Server (JS), it has to check the $DevEUI$ as it would be a normal LoRaWAN message to check if it belongs to a registered LoRaWAN device. If it is not, before discarding the message, which is what will happen in a normal LoRaWAN network, the LoRaWAN NS can checks if the *JoinRequest* contains the extra $RAND$, $AUTS$ and RES fields. These fields could be ciphered by the USIM using the K_i key, thus they only could be decrypted by the UDM, which is the other entity that shares the shared key and the entity responsible for validating them. It is worth to mention that the LoRaWAN specification identifies the type of LoRaWAN messages by using the $MType$ field of the $MHDR$ header available in the LoRaWAN message. We propose to make use of the reserved bits to allow the LoRaWAN JS to identify if it is a normal *JoinRequest* or an extended 5G authentication request. If it is the second one, it has to process the package as a 5G-LoRaWAN roaming message. In such a case, first the JS check the $DevNonce$ to make sure the JS is protected against reply attacks. After that, the *JoinRequest* that contains the 5G SUPI identifier in the place of *DevEUI* field is processed so that the JS can check if the SUPI corresponds to both valid Mobile Country Code (MCC) and Mobile Network Code (MNC). These two values available inside of the $SUPA$ will allow the JS to identify what 5G network operator this device belongs to. Then, the JS will see in its configuration file if there is a trust relationship with such 5G operator. If it is the case, it will contact such operator. But even if it is not the case, the JS can either reject the request or ask a predefined trusted 5G operator. Both cases will be treated equally but the second one will perform the authentication of the 5G credentials using the globally standardized roaming capabilities of the 3G, 4G and 5G networks. In any case, the information available in the *JoinRequest* received by the Join Server and sent to 5G AUSF back-end using a secure channel. To be concrete, we are using the standardized diameter protocol (S6a interface), which is the same interface

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

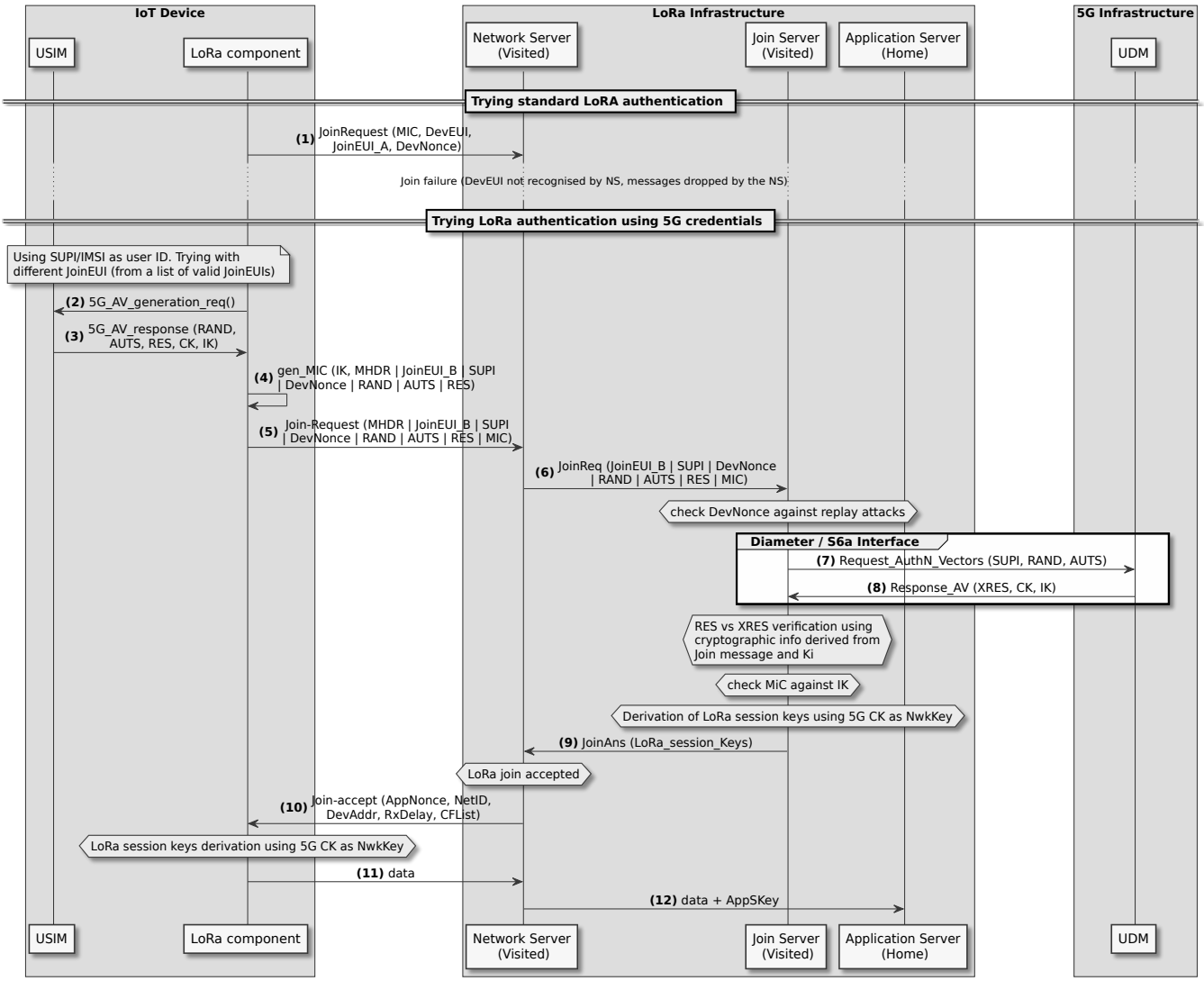

FIGURE 6. Proposed Flow diagram of LoRaWAN authentication using only 5G credentials (Approach A).

being using in the 5G back-end. Messages 7 and 8 shows such message interchange. To carry out this exchange, it has been necessary to define two new messages to consult the UDM, a Request Authentication Vector message (8) that include the params required by the UDM to carry out the authentication of the user in the network $SUPI$, $RAND$, $AUTS$ and the Response AV (Authentication Vector) message (9) to obtain the answer with the $RAND$, $XRES$, $AUTN$, CK and IK fields. When message 8 is received in the UDM, the standard authentication protocol is used with the only exception that traditional the $RAND$ value is generated by the UDM, and in this case it is provided as parameter to the UDM. The answer does not requires to send the $AUTN$ and $RAND$ to the JS so that only $XRES$, CK and IK and sent back to the JS to minimize the exposure of information.

The *JoinRequest* MIC field is used to authenticate and validate the message. It is kept in the JS without being sent to the UDM service until the response obtained from the UDM is received. If the RES generated by the IoT and available in the *JoinRequest* matches the value provided by the UDM in the $XRES$ field, then it is proved on the one hand that the 5G user is who claims to be and knows the corresponding 5G CK and IK sessions key. At this moment, the JS knows both CK and IK session keys and can use the IK to perform the validation of the MIC. It will prove also to the JS the possession of a secure key to be used in the LoRaWAN Network to encrypt messages. Notice that at this state, it has been decided to add an extra layer of security over the existing LoRaWAN security but not making use of such IK and instead make use of the other 5G key CK to encrypt any further messages. Thus, the approach is to make use of the CK as LoRaWAN Network Key. This will also validate that the algorithm generated is 5G compliant.

Message 9 contains the answer from the JS to the NS with the session keys (CK as $NwkKey$). At this point the *JoinRequest* is accepted and the IoT device's security net-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

work data are generated by the NS using standard LoRaWAN security. To be concrete, the device derives the session keys ($FNwkSIntKey$, $SNwkSIntKey$ and $NwkSEncKey$), with aes-128, using as baseline the predefined $NwkKey$ root keys. The network does the same and includes other data such as $NetID$, $DevAddr$, $AppNonce$, $RxDelay$ and $CFList$, which are transmitted to the LoRaWAN device using the $JoinAccept$ message (10). Finally, messages 11 show the IoT device successfully having access to the visited LoRaWAN network thanks to the architecture proposed. However, when the data arrives to the NS, it faces another challenge that need to be addressed. The packet needs to react the appropriate application server into the home network. To address this challenge and take the profit that the 8-bytes $JoinEUI$ field follows a hierarchical addressing using IEEE EUI64 specification. We propose to make use of the 4 first bytes to encode the destination IP address of the Application Server whereas the other 4 last bytes are used to identify uniquely such application inside of the server. This way packets will arrive to the home Application Server encrypted using the associated key and thus they can be decoded and processed accordingly.

C. APPROACH B: NON STAND ALONE LORA-5G CONNECTIVITY

The starting point for this use case is an IoT device with both interfaces LoRaWAN and 5G that has moved to or been deployed at a new/visited LoRaWAN network where there is not LoRaWAN roaming agreements between the visited network and the home LoRaWAN network. The IoT device has also a 5G interface available, which is running and connected to its 5G network. Authors propose to use the 5G credentials and the session keys derived from the active 5G connection to authenticate the device through the LoRaWAN network against the 5G back-end infrastructure.

This proposal offers a simpler integration but imposes stronger requirements such as the dual coverage of both 5G and LoRaWAN at the moment of the authentication in the network. The sequential steps involved in this use case look similar to those presented in the previous section, but in fact, are significantly different in their design.

Figure 7 depicted the sequence diagram of this use case. The first message represents the exchange made between the IoT device through its 5G interface and the 5G infrastructure, to obtain connectivity using the standard *attach* and *connect* mechanisms, that allow to establish an active session between the device and the 5G network.

After the successful authentication in the 5G network, the IoT device tries to connect to a visited LoRaWAN network (Message 2), and the device does not have a valid LoRaWAN credential for that network. This entails an authentication failure, since the device is not recognized by the visited network and there are no roaming agreements between the visited LoRaWAN network and the home network. Then, the hybrid roaming authentication is activated to make use of 5G credentials and session cryptographic material to authenticate the IoT device into the LoRaWAN network.

In this approach, the usage of the USIM functionalities is significantly reduced with respect to approach A to almost their standard use. Hence, the USIM and 5G network are already synchronized due the existing session. Second, there is no need to generate both $RAND$ and $AUTN$ in the USIM for authentication purposes and there is also no need to generate $AUTS$ for synchronization purposes. It makes messages 3 and 4 now much more simplified with respect to the previous approach. To be concrete, Messages 3 and 4 are sent internally between the IoT device the USIM to obtain the 5G identifier (SUPI/IMSI/SUCI) and the cryptographic information (session keys - CK and IK). As seen above, the authentication of a LoRaWAN device is done through the validation of the MIC field of the LoRaWAN *JoinRequest* message header, generated in step 5. Now, the format of this *JoinRequest* is fully compliant with the standard one since there is not any need to pass any extra $RAND$, $AUTS$ and RES information in the message due to the existing 5G session.

The calculation of the MIC is also following the standard procedure with the only difference that it is making use of the 5G IK as a key to perform the generation of the MIC instead of the original LoRaWAN $NwkKey$. It makes a significantly easier integration. The standard LoRaWAN *JoinRequest* have three fields: $DevEUI$, $JoinEUI$ and $DevNonce$. It is necessary to replace the LoRaWAN $DevEUI$ identifier with the $SUPI$, which internally have a specific format and allows to recognize that identifier as a 5G own one and it will allow to activate the roaming as well as subsequently resend the package to the corresponding 5G back-end.

The logic of the LoRaWAN JS is exactly the same as the one indicated in the previous use case (messages 6 and 7) but Message 7 and 8 that imply the interaction with the 5G architecture are different. Now, the AUSF and UDM have already done a standard 5G authentication. It implies that AUSF have in memory both CK and IK from the authentication vector received by UDM. Therefore, we propose the addition of a new method in the API of the AUSF called: $Request\_LoRa_AuthN$, accessible through the S1AP NAS interface, that receives all the information available in the *JoinRequest* that is required to create the $XMIC$ (MIC generated by AUSF) together with the MIC value available in the *JoinRequest*. Then, AUSF will make use of the IK to perform the creation of such $XMIC$. As a result, if they both matches, means that both ends of the communication have a proof of possession of the IK. Only if there is a match, Message 10 returns the $XMIC$, CK and IK to the join server. This will allow the Join Server to check the $XMIC$ against the MIC received in the *JoinRequest*. Notice that this match has been already done by the AUSF but here the process is again done since the Join Server needs also to demonstrate such proof of possession now for the LoRaWAN network. If they match, then as an extra security layer, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

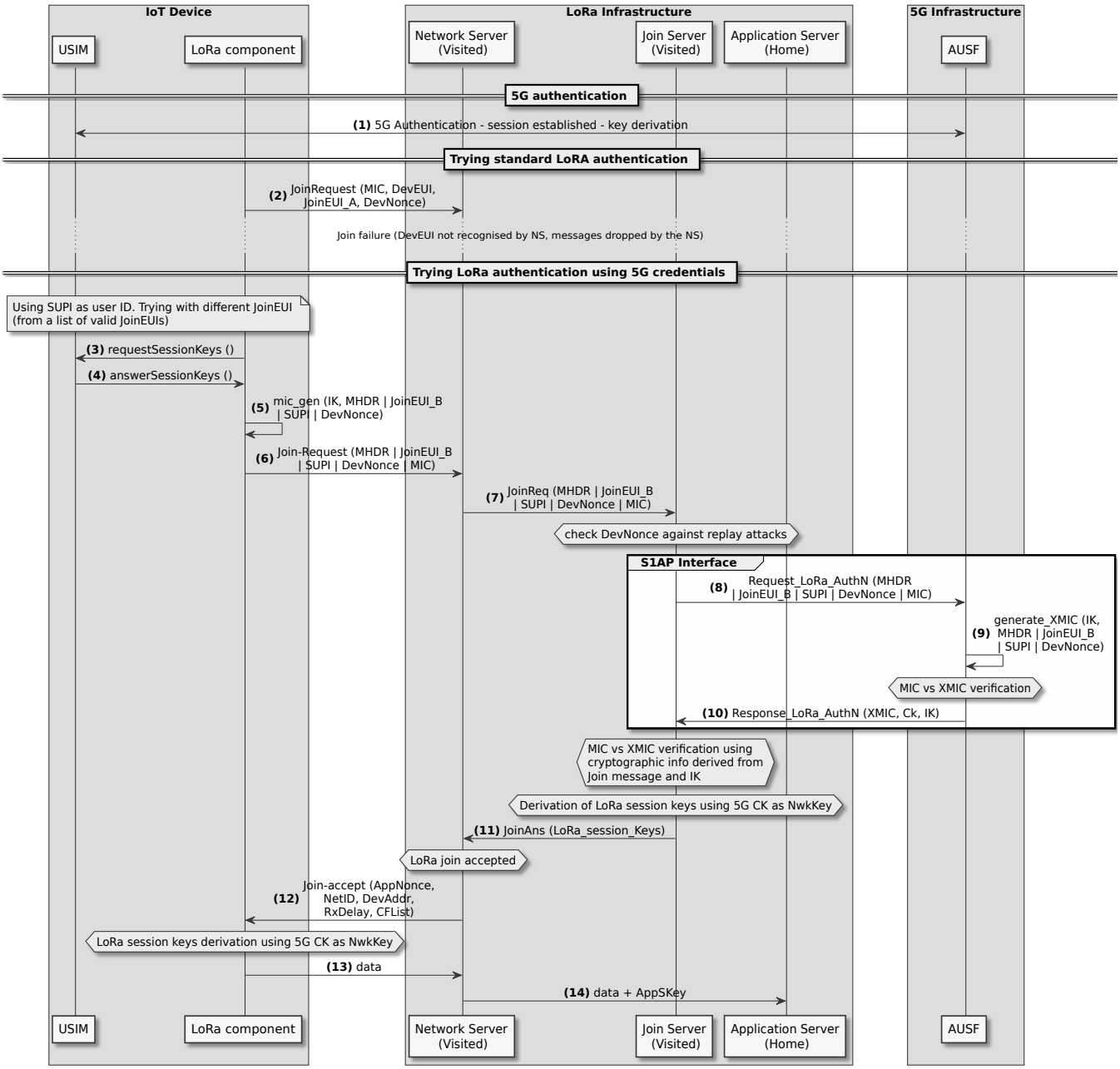

FIGURE 7. Proposed Flow diagram of LoRaWAN authentication using 5G derived keys (Approach B - 5G pre-authentication)

The rest of the process will be carried out in the same way as the described in approach A. Notice that this approach makes use the 5G CK as a LoRaWAN $NwkKey$, similarly to the other approach presented. And, the IoT device will derive session keys ($FNwkSIntKey$, $SNwkSIntKey$ and $NwkSEncKey$), with aes-128, using as baseline the predefined $NwkKey$ root keys.

D. COMPARATIVE ANALYSIS OF THE PROPOSED ROAMING APPROACHES

This section provides a comparative analysis of the two different proposals previously described. A summary of such comparison is shown in table 1. As the reader can see, approach B is significantly following almost all the standard procedures and the only requirements to extend the S1AP interface with a new functionality to calculate LoRaWAN MIC using internal cryptography material available by the AUSF however, the main drawback is the need of the dual coverage in the moment of the authentication. Approach A is able to remove such limiting requirement but imposes a significant deviation of the standards in both LoRaWAN and 5G networks with the drawbacks imposed in terms of the adoption by industry, especially in terms of firmware optimization, hardware feature implementation and software

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

APIs. It also required a deeper security analysis, described later on. For these reasons, authors have decided to carry out the security analysis for both approaches to ensure correctness of the solution but to perform the empirical validation of the architecture proposed only on approach B.

Feature	Approach A	Approach B
Standard LoRaWAN MIC Calculation	NO	YES
Standard LoRaWAN JoinRequest Message	NO	YES
Required Dual and Simultaneous Coverage Anytime	NO	NO
Required Dual and Simultaneous Coverage at Authentication Phase	YES	NO
Standard USIM Cryptography Functions	NO	YES
Standard s6A Interface	NO	YES
Standard S1AP Interface	YES	NO

TABLE 1. Comparison between different approached proposed

VI. SECURITY ANALYSIS OF THE PROPOSED ROAMING APPROACHES

In this kind of interoperability scenarios in which situations of integration of protocols, infrastructures and organizations arise, security can be affected in different aspects. At organization level, because new trust relationships have to be established between the involved organizations. At infrastructural level, services may require new trust relationships based on service enrolments, certificates and new interconnection interfaces. Finally, at the protocol level, interoperability solutions usually require changes at different depths, modifying the uses of the exchanged messages and the information transported in them, as well as the definition of new messages to adapt to the requirements of each case of use.

The designed interoperability solution between LoRaWAN and 5G, has been performed minimizing the changes in the existing standards. The changes mainly affect client devices and the infrastructure responsible for authentication, leaving intact, in most cases, intermediate components in charge of the exchange of messages in data and control planes.

The two proposed solutions share common modifications that can affect different security aspects that must be taken into account. Next, the changes carried out by the proposed solutions and the decisions taken to minimize security and privacy risks are analysed.

A. JOIN-REQUEST AS PLAIN TEXT

LoRaWAN standard authentication is done through the *JoinRequest* message, which is the first message sent by the LoRaWANdevice to the Network Server in order to establish the connection and authenticate the device. This message, sent in clear text, contains mainly the $JoinEUI$, $DevEUI$ and $DevNonce$. These fields, along with others, are processed in the MIC function to verify the integrity of the message. For this, the shared secret key $NwkKey$ is used, which allows also verifying that whoever generated that MIC results corresponds to the $DevEUI$.

Thus, in our approach A, it is also sent in the same *JoinRequest* both $RAND$, $AUTS$ and RES. These fields are provided with the only purpose of verifying the proof of possession of K_i and the associated derived CK and IK keys, which are used then to authenticate such IoT device. Thus, if a malicious attacker has access to this plain text message, he cannot perform a reply attack since the $DevNonce$ have been already consumed by the legitimate request. Besides, if the attacker might want to change such $DevNonve$ value, then the MIC cannot be recalculated since he is not in a possession of the IK. Therefore, authors do not foresee any concern to this approach. However, we have proposed an extra protection, to encrypt them using the K_i so that only UDM service can decrypt it. This implies an enhanced privacy solution where reply attack will not feasible.

B. SUBSCRIPTION PERMANENT IDENTIFIER (SUPI) PROTECTION

To identify the 5G user in the LoRaWAN infrastructure, such 5G SUPI/IMSI identifier needs to be transmitted instead of the LoRaWAN identifier. It can involve a security and privacy risk [30] since the SUPI/IMSI is recommended to be encrypted in 5G even when it is not done in 4G and it will be exchanged in LoRaWAN network inside of the LoRaWAN *JoinRequest* message without encryption. To cope with this issue, our proposal encrypts the 5G SUPI/IMSI identifier during the LoRaWAN packets transmissions using the 5G shared key (K_i).

According to the 5G specification, the SUPI/IMSI identifier is, in general, never sent in clear text over the radio 5G network, being this feature considered a major security improvement over prior generations such as 4G. Nevertheless, there are certain situations where authentication through the use of temporary identifiers is not possible. For instance, when a user registers with a network for the first time and is not yet assigned a temporary identifier. In this case, and even more in roaming scenarios, is not possible to use a temporary identifier.

The mechanism defined by the 5G standard is the use of the Subscription Concealed Identifier (SUCI). This identifier is a privacy preserving identifier containing the concealed SUPI. In 5G, the UE generates SUCI using a ECIES-based protection scheme with the public key of the Home Network that was securely provisioned to the USIM during the USIM registration. Only the MSIN part of the SUPI gets concealed by the protection scheme while the home network identifier, the MCC/MNC, gets transmitted in plain text. In the proposed solution, the protected part of SUCI is ciphered using the 5G shared key (K_i), which only allows the disclosure by the 5G back-end.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

These attacks are known as *IMSIcatching attacks* [31] and persist in today's mobile networks 4G LTE/LTE+ [32]. The use of SUCI is compatible with our both approaches and aligns the solution to the last security recommendations of 5G specification.

C. MULTIPLE KEYS AS LORAWAN NETWORK KEY

It is worth mentioning that both proposed integration approaches make use of the stronger security mechanisms available in 5G to provide an extra layer of security over the LoRaWAN network. It is done by employing not only one $NwkKey$ but using CK and IK as two different $NwkKey$. Thus, IK is used only for the *JoinRequest* (MIC calculation) and the CK for any other message and session key derivations. It enhances significantly the changes to get keys compromised.

D. MUTUAL AUTHENTICATION

In terms of mutual authentication and trust relationships: i) IoT device needs to get authenticated in both, the visited LoRaWAN network (JS) and in 5G network (AUSF/UDM). ii) JS need to authenticate both, IoT and 5G network. And iii) 5G network need to authenticate both the JS and IoT device.

Regarding mutual authentication IoT-5G, it will make use of the standard mutual authentication mechanisms for approach B. In approach A, however, this is carried out by the generation of the $XMIC$ in the AUSF and its validation against the MIC provided in the authentication request received by the JS.

With regard to JS-(UDM/AUSF) mutual authentication and encryption, this is carried out by the creation of a secure channel (TLS) where there is a mutual authentication based on a PKI infrastructure and x.509 certificate in both client (JS) and server (UDM/AUSF) side. It allows both encryption of the communications and mutual authentication, using standard mechanisms.

With respect to IoT-(visited JS) mutual authentication, JS completely relies on the 5G network to provide a trusted IK and CK to allow JS to authenticate IoT devices. This trust relationship is a key aspect of the proposed architectures. Security is addressed previously with the usage of the mutual authentication between JS and UDM/AUSF and a secure channel as previous discussed. IoT device authenticates the network since messages exchanged thereafter are encrypted with the $NwkSKey$ session key only known by the NS that uses it as proof of possession, thereby guarantying that Network server is trusted.

The implications of this trust relationship between JS and AUSF/UDM is that JS will allow to pass messages across its network based on such trust relationship. However, notice that to allow this to happen, the IoT device and its possession of the IK and CK need to be successful along the authentication process.

In the proposed Approach A, $RAND$, $AUTS$ and RES are generated in the USIM so that the USIM has not really authenticated the 5G infrastructure, but notice that in fact the IoT device does not plan to connect and maybe does not have even coverage. Thus, this is not any security concern with respect to the 5G network.

E. KEYS SHARED BETWEEN AUSF/UDM AND JS

In traditional 5G authentication, the K_i is the master key provisioned inside of the USIM that never goes out of the USIM. However, both CK and IK session keys are transferred to the IoT Device without any mayor security concerns since the PIN code has been already being used to authenticate access to such keys. In the information exchange between AUSF/UDM and JS these keys are also being shared between. There is not any mayor concern (similarly as with the USIM approach) to share such keys between them. However, a mechanism similar to the USIM should be provided from the infrastructure side. To address this, a dual layered security mechanism has been proposed. First a PKI-based secured channel (TLS) with dual authentication in place. And second, the validation of the MIC received as a initial proof of possession of the K_i without unveiling any further information. This is the reason why the MIC is passed to AUSF/UDM so that this validation can be done before to share any session key with JS. Obviously, the K_i will never go outside of the 5G UDM which is what is expected to be, following standard 5G security architecture.

F. REPLAY AND DDOS ATTACKS

With respect to replay attacks against the standard LoRaWAN architecture, LoRaWAN uses a random number created by the EDs ($DevNonce$). It is used to circumvent replay attacks during the authentication phase.

NS keeps the list of used ($DevNonces$) and automatically protects the network from the re-usage of the same $DevNonce$. As a result, any DDoS attack using the same $DevNonce$ will also be mitigated. However, an advanced DDoS could be smart enough to generate a different $DevNonce$ for each *JointRequest*, then NS will not ignore such messages and the flooding will be received in the JS that, in turn, will provide a negative authentication based on the MIC value and the fact that the attackers do not know the $NwkKey$.

In our approaches, it will also produce an overhead in AUSF (approach B) or UDM (approach A) even time JS is being attack. In summary, the amount of traffic that can be injected in the network for authentication purposes until the device received a permanent denial is 2^16 being 16 the number of bits used for the $DevNonce$. After that, it will be a lack of any non-used $DevNonce$ and NS will stop such DDoS. Thus, the maximum amount of traffic generated by a malicious traffic is exactly $65536 * 23$ being 23 the standard size of the *JoinRequest*, totalling a maximum of 1.5 MBytes. This is a clear method to control this risk, but authors also propose to have a maximum number of a configurable roaming access attempt before to stop passing request to the UDM and AUSF. e.g. 3 times in a minute. Thus, this is a simple mechanism to be addressed by the NS

in order to keep the number of *JoinRequest* received in the last X seconds from a device and drop any further attempt.

Another aspect to analyse is the reason why AUSF/UDM will also receive such attack when the JS is being attacked. The reason is that JS (in roaming) does not have yet any key to check MIC before to do the request to AUSF/UDM, thus it needs to pass always such message, but again the attack can be controlled, as already explained.

VII. IMPLEMENTATION AND VALIDATION

In order to validate the feasibility of the proposed solution, a Proof of Concept (PoC) implementation has been carried out focusing on the second approach defined in (Section V-C). Additional instrumentation has been included to gather metrics to perform evaluation.

As explained in Section V-D, Approach B has been chosen for implementation and validation, since it better aligns with existing standards, requiring only small changes at the LoRaWAN specification level and minor modifications at the service adaptation level.

The PoC has been developed using software at production level such as Mosaic 5G [33] for the 5G infrastructure and ChirpStack/Broocar [34] for the LoRaWAN infrastructure. There is not any modifications at the hardware level in any of the devices involved in the infrastructure, which facilitates the reproducibility of the tests carried out, explained in more detail in sections B and C of this section.

Section A describes the testbed where the validation has been carried out. After that, Section B. provides the process that has been carried out to perform the validation of the approach. Then, Section C. describes the results of the execution of such validation process. These results include the execution of each of the steps involved in a complete execution of authenticating an IoT device with LoRaWAN and 5G interfaces in accessing a LoRAWAN network using 5G credentials. Finally, Section D provides a detailed analysis of different metrics to evaluate the communication cost, effectiveness, overhead and viability.

A. IMPLEMENTATION AND TESTBED DESCRIPTION

Figure 8 depicts the whole architecture deployed in our premises. It is a dual architecture that includes both LoRaWAN and 4G/5G components. Both architectures have several components that are virtualized and deployed as Virtual Network Functions (VNFs) in different physical machines. All the Virtual Machines have been defined with the same configuration: CPU Intel Core Processor (Broadwell) 64 bits, RAM 2GB, HD 20 GB and Ubuntu 16.04 kernel 4.15.0 low-latency.

With respect to IoT devices, we are using a Pycom Fypi ESP32 device with WIFI, Bluetooth LoRa, Sigfox, LTE CAT M1/NB1 interfaces. This device have a SPI interface to the LoRaWAN interface and a UART interface to the 5G NB-IoT interface. The firmware v1.17.3.b1 has been customized including an ad-hoc LoRaWAN client written in micropython that interacts with the UART NB-IoT interface to connect to the 5G network and to recover. It uses AT commands over UART both SUPI/IMSI and session credential information (CK and IK) to be used as $NwkKey$ for the LoRaWAN modem when requested. The micropython API allows to interact with the USIM at low level, necessary to manage the access to the cryptographic material. This part has been made using as baseline the Osmocom [35] open source libraries [36] [37] that offers both, client and infrastructure functions very appreciated for our purpose. These credentials are used to replace the $DevEUI$ and to calculate the MIC using the IK. The code that interacts with the USIM is based in the Osmocom libraries [35]

Regarding the LoRaWAN network, the LoRaWAN gateway is an standard Raspberry Pi 2 with a IC880 hat to provide a LoRaWAN interface. It has been installed with the Chirpstack/Brocaar LoRaWAN Gateway software, the Packet Forwarder (poly_pkt_fwd). The LoRaWAN NS is a VNF using in EDGE-1 zone of OpenStack (cloud computing stack), and with Chirpstack/Brocaar LoRaWAN Network Server (bridge) and Mosquitto MQTT v3.1.1. The LoRaWAN AS and JS are both integrated in the same software, the Chirpstack/Brocaar LoRaWAN Application Server. This code has been modified to identify roaming messages from the IoT device and, in case of roaming process, being able to contact with 5G AUSF component to delegate the validation of the LoRaWAN *JoinRequest* message.

Regarding the 5G Networks, the Radio Access Network has been prototyped using a Ettus URSP B210 SDR running the UHD firmware v3.9 and Mosaic 5G v1.0 running in a VNF using EDGE-2 zone of OpenStack. Both AUSF and UDM has been installed using the NextEPC Core network components [38] (MME and HSS, respectively) due to the limitation, that there is not any open source implementation of a 5G core network available to perform the validation. However, all these principles are directly applicable to the new 5G core network. Figure 8 does not show the rest of 5G components for a shake of simplicity, however, 5 different VNF are deployed in the CORE of the network with all the architectural components of the 5G network. Both AUSF/-MME and UDM/HSS have been modified according to the approach B presented in previous sections.

B. VALIDATION PROCESS

For the validation of the approach, we have implemented a proof of concept of the Approach B previously presented, allowing a FiPy IoT device being authenticated into the visited LoRaWAN network using the CK and IK session keys. To allow so, a new micropython API has been implemented that permits extracting the IK nd CK session keys as well as the $SUPI$ from the IoT device to be used. The client can access to them after the connection to the 5G network has been carried out and be used as $NwkKey$. Namely, the prototype makes use of the IK for the MIC calculation of the *JoinRequest* whereas makes use of the CK for the LoRaWAN session keys derivation used for the MIC calculation of the rest of messages.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

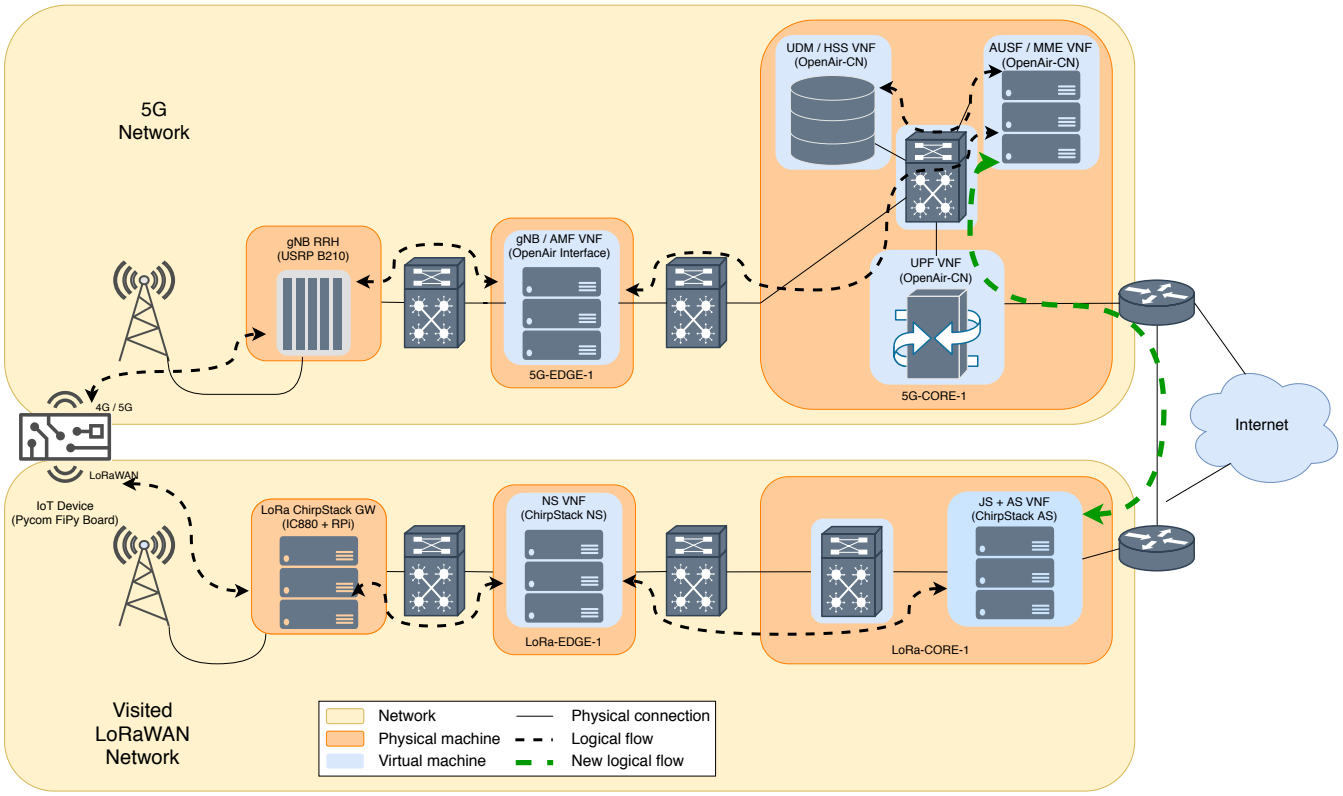

FIGURE 8. Diagram of the implemented LoRaWAN and 5G integration testbed

The Join Server is the component in charge of validating the *JoinRequest* messages. The PoC has been implemented using the LoRaWAN library offered by Chirpstack/Brocaar. The modifications have been focused in the LoRaWAN library, which is in charge of managing and validating LoRaWAN messages such as *JoinRequest* message. To be concrete, it has been modified the case where a unknown DevEUI is received in a *JoinRequest*, checking whether the format of the received identifier matches with the SUPI/IMSI format by extracting both MNC and MCC and checking them against a list of pre-configured IP address where the 5G AUSF is available for such 5G network. It that case, the roaming protocol is activated sending the request against AUSF. This has been the most challenging part of the integration. It has required to perform the extension of the API exposed by the AUSF/MME in order to offer two new methods in its S1_AP interface, matching the signature indicated in Figure 7. Although the defined solution maintains the use of the S1AP interface for the validation of the message received from the LoRaWAN Join Server, it is necessary not only to implement the new request-response pair of interactions. Probably the most complex aspect of this integration has been the creation of the S1AP client library to interact with the AUSF inside of the JoinServer. Notice that LoRaWAN implementation is carried out in GO language whereas 5G implementation is carried out in C/C++ language.

For demonstration purposes, the implementation of the AUSF API has intentionally ignored many of the S1AP checks indicated in the standard and only focused on validating the approach. Obviously, on production stage, all these standard checks should be implemented. Upon returning to the LoRaWAN Join Server, the stored *JoinRequest* fields are retrieved and the preceding MIC from the IoT device is compared with the $XMIC$ provided by the 5G infrastructure. If they match, the LoRaWAN device is successfully authenticated and normal LoRaWAN operation proceeds.

C. EXECUTION

In terms of the cryptography used to carry out such authentication, and as a proof of validation, our SIM card has been intentionally reprogrammed with this cryptography information generated for this validation purposes.

KI=$0x89423C6213B1762E5D96CF1756E929BD$
SUPI=809901700000020498
($0xB3D594E1B7C7812$)

Information presented here in is accurate so that it will allow any reader to reproduce the validity of the approach B described in this contribution. As a result of the 5G authentication, it has been generated:

IK = $0xC295253CA52E58BA43228C380C86FEC1$
CK = $0x57B352B81939C178863E63f90EADCB78$
RES = $001fA4d4AC200DAB$

Then, LoRaWAN information available in the *JoinRequest* is the following:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

MHDR = 0x00 (*JoinRequest*),
AppEUI = 0x0000000000000001,
DevEUI = 0x00B3D594E1B7C781,
DevNonce = 0x15A1 (randomly generated).

Notice that $DevEUI$ is made with the $SUPI$ identifier in hexadecimal and with padding to fit into the size of the field. These field produces the following MIC as an output: MIC=$1E01652E$. XMIC produced by AUSF is exactly the same value validating the feasibility of the presented solution.

D. VALIDATION ANALYSIS

The execution of the whole authentication process has been carried out in different scenarios to allow comparison between them. This process has been instrumented to gather some key metrics to allow the analysis of the overhead proposed by our solution. To be concrete, three different scenarios has been executed, including traditional LoRaWAN authentication in local networks, and roaming using our approaches. Table 2 summarises the validation results obtained along the tests carried out as proof of concept with the aim of analyse the communication cost and overhead inserted by the proposed approach.

In terms of overhead, approach A introduces an overload in the size of Join Request message since it is necessary to transport three new additional fields ($RAND$, $AUTS$ and RES). This implies an increase of 38 bytes over the standard message size which is 23 bytes. This increment is not a problem since the new size is supported by the LoRaWAN standard. On the other hand, approach B does not have impact in the size of Join Request message as shown in Table 2.

Additionally, the effect introduced by the delegation on a third party such as the 5G back-end of the LoRaWAN authentication process implies a series of additional hops between components and additional cryptographic calculations with the consequent delay associated. A standard LoRaWAN authentication requires four hops to complete the device authentication process. The proposed solutions imply an additional access to 5G back-end, adding an extra request/response exchange, leading to six his required in total to complete the authentication. It is worth to mention that approach B required that the authentication of the device in the 5G network is also previously carried out with an additional four hops.

To take time measurements between the different packages, modifications have been made to the LoRaWAN Gateway. The measurements are not made in the IoT device itself since the sending and receiving windows are delimited and fixed in advance by the LoRaWAN standard. A normal authentication in a home LoRaWAN network takes 10ms in our setup, whereas it takes 14ms in a visited LoRaWAN network, which gives an idea of the small overhead introduced in the control plane, i.e. 4ms. Besides, there is not any additional overhead in terms performance in the data plane since it has not been modified.

TABLE 2. Validation results analysis. Joint Request (JR)

	Hops	Time	JR Packet Size
Standard LoRaWAN	4	10 ms	23 B
Aproach A	6	-	61 B
Aproach B	6*	14 ms	23 B

To ensure the low energy and resource consumption required in IoT networks, the LoRaWAN specification defines two very short receive windows, aimed to obtain the response messages each time the device is activated (either to send an update or register in a new network). In the case of the *JoinRequest* authentication message, as defined in LoRAWAN Regional Parameters [39], the maximum delay to receive the $JOIN\_ACCEPT$ is 5-6 seconds. The 4ms of overhead associated to our approach is minimal compared to such standard reception windows, which makes the approach suitable for LoRaWAN standard and does not impose any additional energy consumption.

VIII. CONCLUSION

This paper has defined the first novel proposal aimed to enable handover roaming in LoRaWAN by relying on 5G security services. To this aim, two different approaches to achieve the integration of LoRaWAN and 5G have been exhaustively detailed, analysed and compared. The first approach, based on extending LoRaWAN join procedures for piggybacking 5G security material, is intended to allow roaming in LoRaWAN with 5G authentication. This solution does not require 5G coverage in the visited LoRaWAN network, but several modifications in the LoRaWAN and 5G standards are needed. On the other side, the second approach, based on exploiting 5G authentication services, has been selected for implementation and validation, since it follows almost all the standard procedures with minimal modifications. This approach has been successfully implemented, with the required developments for the IoT device (including in the 5G SIM card part), in the LoRaWAN Join Service as well as in the 5G AUSF to perform the 5G authentication as detailed in the paper. The implementation, deployment and validation of the approach in a real integrated LoRaWAN and 5G testbed, as well as the conducted security analysis has shown the feasibility of the proposal. As future work, we envisage to devise additional novel trusted security procedures for mobility and roaming aimed to cope with interoperability issues between 5G and other IoT wireless network protocols.

ACKNOWLEDGMENT

This work has been funded by a grant for postdoctoral training and improvement abroad, funded by the Ministry of Employment, Universities, Enterprise and Environment of the CARM (20938/PD/18), through the Seneca Foundation-Agency for Science and Technology of the Region of Murcia (Spain). This work has been also partially supported by the European Commission H2020 5G-PPP ICT-2016-2 SliceNet

project GA 761913, as well as H2020 European project INSPIRE-5Gplus GA 871808.

REFERENCES

[1] C. Bockelmann, N. Pratas, H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski, and A. Dekorsy, "Massive machine-type communications in 5g: physical and mac-layer solutions," IEEE Communications Magazine, vol. 54, pp. 59–65, Sep. 2016.

[2] EGHAM, "Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020," 2019.

[3] L. A. T. Committee et al., LoRaWAN 1.1 Specification.

[4] J. C. Zuniga and B. Ponsard, "Sigfox system description," LPWAN@ IETF97, Nov. 14th, vol. 25, 2016.

[5] M. Vaezi, Z. Ding, and H. V. Poor, Multiple access techniques for 5G wireless networks and beyond. Springer, 2019.

[6] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3gpp narrowband internet of things," IEEE communications magazine, vol. 55, no. 3, pp. 117–123, 2017.

[7] C. Bockelmann, N. K. Pratas, G. Wunder, S. Saur, M. Navarro, D. Gregoratti, G. Vivier, E. De Carvalho, Y. Ji, Ä. StefanoviÄĞ, P. Popovski, Q. Wang, M. Schellmann, E. Kosmatos, P. Demestichas, M. Raceala-Motoc, P. Jung, S. Stanczak, and A. Dekorsy, "Towards massive connectivity support for scalable mmtc communications in 5g networks," IEEE Access, vol. 6, pp. 28969–28992, 2018.

[8] A. Lavric and V. Popa, "Internet of things and loraâĎć low-power wide-area networks: A survey," in 2017 International Symposium on Signals, Circuits and Systems (ISSCS), pp. 1–5, 2017.

[9] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," ICT Express, vol. 5, no. 1, pp. 1 – 7, 2019.

[10] A. SEMTECH and M. Basics, "An1200. 22," LoRa Modulation Basics, vol. 46, 2015.

[11] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015.

[12] K. Mikhaylov, J. Petajajarvi, and J. Janhunen, "On lorawan scalability: Empirical evaluation of susceptibility to inter-network interference," in 2017 European Conference on Networks and Communications (EuCNC), pp. 1–6, June 2017.

[13] I. Butun, N. Pereira, and M. Gidlund, "Analysis of lorawan v1. 1 security," in Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, p. 5, ACM, 2018.

[14] LoRa Alliance Technical Committee and others, LoRaWAN Back-End Interfaces v1.0. LoRa Alliance, 5177 Brandin Court. Fremont, CA 94538, 1.0 ed., 10 2017.

[15] ETSI, "5g; security architecture and procedures for 5g system (3gpp ts 33.501 version 15.1.0 release 15)," tech. rep., jul 2018. DTS/TSGS-0333501vf10.

[16] GSM Association, "5g roaming guidelines, version 1.0."

[17] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5g mobile wireless networks," IEEE Access, vol. 6, pp. 4850–4874, 2018.

[18] T. S. G. Services and S. Aspects, "System architecture for the 5g system (5gs) - 3gpp ts 23.501 version 16.3.0 release 16, stage 2," tech. rep., dic 2019.

[19] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, "The Network Access Identifier." RFC 4282, Dec. 2005.

[20] T. S. G. C. Network and Terminals, "Numbering, addressing and identification - 3gpp ts 23.003 version 16.1.0," tech. rep., dic 2019.

[21] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements and future directions," IEEE Communications Surveys & Tutorials, 2019.

[22] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," IEEE Access, vol. 6, pp. 3619–3647, 2017.

[23] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of lorawan and 4g/5g for the industrial internet of things," IEEE Communications Magazine, vol. 56, pp. 60–67, Feb 2018.

[24] R. Yasmin, J. PetÃď'jÃď'jÃď'rvi, K. Mikhaylov, and A. Pouttu, "On the integration of lorawan with the 5g test network," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–6, Oct 2017.

[25] A. Neumann, L. Wisniewski, T. Musiol, C. Mannweiler, B. Gajic, R. S. Ganesan, and P. Rost, "Abstraction models for 5G mobile networks integration into industrial networks and their evaluation," pp. 88–101, 2020.

[26] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')." RFC 5448, May 2009.

[27] D. Garcia-Carrillo, R. Marin-Lopez, A. Kandasamy, and A. Pelov, "A coap-based network access authentication service for low-power wide area networks: Lo-coap-eap," Sensors, vol. 17, no. 11, 2017.

[28] E. Pearce and E. Lawson, "Lora alliance passes 100 lorawanâĎć network operator milestone with coverage in 100 countries," 2019.

[29] J. Koon, LoRaWANÂő Empowers Very Low-power, Wireless Applications: The Future of Low-power Wireless Network. "Lora Alliance", nov 2019.

[30] H. Khan, B. Dowling, and K. M. Martin, "Identity confidentiality in 5g mobile telephony systems," in Security Standardisation Research (C. Cremers and A. Lehmann, eds.), (Cham), pp. 120–142, Springer International Publishing, 2018.

[31] A. Lilly, "Imsi catchers: hacking mobile communications," Network Security, vol. 2017, no. 2, pp. 5 – 7, 2017.

[32] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," p. 16, 01 2016.

[33] M. G. Consourtium, "Mosaic5g web portal." http://mosaic-5g.io, 2020. Accessed: 2020-01-25.

[34] O. Brocaar, "Chirpstack, open-source lorawanÂő network server stack." https://www.chirpstack.io/, 2020. Accessed: 2020-01-25.

[35] J.-P. Lang, "Osmocom web portal." http://osmocom.org/, 2019. Accessed: 2020-01-25.

[36] P. Maier, "Osmocom osmo-sim-auth library." http://git.osmocom.org/osmo-sim-auth/, 2019. Accessed: 2020-01-25.

[37] Osmocom Project, "Osmocom osmo-auc-gen library." https://osmocom.org/projects/osmo-sim-auth, 2012. Accessed: 2020-01-25.

[38] NEXTEPC INC., "Nextepc 5g project." https://nextepc.org, 2010. Accessed: 2020-01-25.

[39] LoRa Alliance Technical Committee Regional Parameters Workgroup, LoRaWAN 1.1 Regional Parameters. LoRa Alliance, Inc, 2400 Camino Ramon, Suite 375. San Ramon, CA 94583, 1.1 ed., 1 2018.

ELENA M. TORROGLOSA GARCIA Elena Torroglosa received the B.S., M.S., and Ph.D. degrees in computer science from the University of Murcia, Murcia, Spain. She has been involved in multiple research projects in diverse fields such as AAA/Identity management (SWIFT, GEMBus, STORK2.0, GN4-1-SA5-T1, GN4-2-JRA3T3, OLYMPUS), design of inter-federation solutions (GN4-1-SA5-T1: STORK2 with eduGAIN, GN4-2-JRA3T3: eIDAS with eduGAIN), ÂăExperimentation Infrastructures such as OpenLAB. Currently, she is currently doing a 2-years stay at the School of Computing, Engineering and Physics Science of the University of the West of Scotland thanks to postdoctoral grant of the CARM (20938/PD/18), through the Seneca Foundation-Agency for Science and Technology of the Region of Murcia (Spain). Her current stay at UWS is focused on the development of advanced identity management systems for IoT devices on 5G networks, using innovative interoperability mechanisms as well as cognitive methods to improve the management of infrastructure, users and services.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2998416, IEEE Access

JOSE M. ALCARAZ-CALERO , Full Professor in Networks at University of the West of Scotland, United Kingdom. He is technical co-coordinator of the EU-H2020 5G-PPP Phase I SELFNET and EU-H2020 5G-PPP Phase II SliceNet projects. Alcaraz-Calero has more than 200 publications in a wide range of professional interests including cognitive pipelines, network management, monitoring and control, automation and orchestration, cyber security, data analytics and computer vision. (jose.alcaraz-calero@uws.ac.uk).

JORGE BERNAL BERNABE received the B.S., M.S., and Ph.D. degrees in computer science as well as the M.B.A. degree from the University of Murcia, Murcia, Spain. He was granted with the Best Ph.D. Thesis Award from the School of Computer Science of the University of Murcia. Currently, he is a Postdoctoral Researcher in the Department of Information and Communications Engineering of the University of Murcia. Jorge Bernal has been Visiting Researcher in the Cloud and Security Lab of Hewlett-Packard Laboratories, Bristol, UK, and author of several book chapters and more than 40 papers in international top-level conferences and journals. He has been involved in the scientific committee of numerous conferences and served as a reviewer for multiple journals. During the last years, he has been working in several European research projects FP7 and H2020, such as DESEREC, Semiramis, Inter-Trust, SocIoTal, ARIES, OLYMPUS, Anastacia, CyberSec4EU or INSPIRE-5GPlus. His scientific activity is mainly devoted to the security, trust, and privacy management in distributed systems. He is also interested in security and privacy aspects in the Internet of Things.

ANTONIO SKARMETA Antonio Skarmeta received his Ph.D. degree in computer science from the University of Murcia, Murcia, Spain, M.S. degree in computer science from the University of Granada, Granada, Spain, and B.S. degree (with honors). Since 2009, he has been Professor at University of Murcia, Murcia, Spain. Skarmeta has worked on different research projects in the national and international area in the networking, security, and IoT area, like Euro6IX, ENABLE, DAIDALOS, SWIFT, SEMIRAMIS, SMARTIE, SOCIOTAL, and IoT6. His main interest is in the integration of security services, identity, IoT, and smart cities. He has been the Head of the research group ANTS since its creation in 1995. He is also an Advisor to the Vice Rector of Research of the University of Murcia for international projects and Head of the International Research Project Office. Since 2014, he has been the Spanish National Representative for the MSCA within H2020. He has published over 200 international papers and has been a member of several program committees. He has also participated in standardization for IETF, ISO, and ETSI.